Cyber Security Incidents Outside Malaysia

Report No. 4 Feb 2007
CONTENTS

FRAUD
1. Combating online fraud 3
2. Internet ID theft scam 3
3. Warning! Online coupon fraud 3
4. Pharming scam 4
5. EU to launch scam crackdown 4

HACK THREAT/INTRUSION
6. Chinese police consider releasing hacker's Panda virus fix Would you run a virus writer's anti-virus? 4
7. Turkish hacker strikes Down Under 5
8. Broadband routers welcome drive-by hackers 5
9. Drive-by Web attack could hit home routers 6
10. Hacking business 6
11. Imperfect Storm aids spammers 6
12. Hackers pounce on Howard 'heart attack e-mail' 7
13. Monster.com email lure to malicious code 7
14. Hackers infiltrate websites 7
15. Vulnerabilities of WiFi Internet 8

VIRUS/WORM/TROJAN
16. Infected PCs spew malware over 3G connections 8
17. Panda virus in China 8
18. Storm Worm variant targets blogs, bulletin boards 9

OTHERS
19. Quake-hit web links restored in Asia 9
20. Computer crime wins the fight 9
21. FSA has power to order data breach disclosure 10
22. Pirates nabbed 10
23. How cybercrime works 11
24. Region faces cybercrime wave 11
25. No jail time for child porn 11
26. CBI calls for Internet security 12
27. Security, consolidation top CIOs' agendas 12

DISCLAIMER

This document is a non-commercial publication intended to educate and disseminate information about security incidents reported outside Malaysia. Further reproduction or redistribution is subject to original copyright restrictions. NISER provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

NISER did not warrant the completeness or accuracy of the document and neither accepts any liability for losses howsoever incurred. The content on this site, including
news, quotes, data and other information, is provided by third party content providers for your personal information only, and neither NISER nor its third party content providers shall be liable for any errors, inaccuracies or delays in content, or for any actions taken in reliance thereon.
1. **Combating online fraud**

Focus has once again fallen on the need to combat online fraud as a Bidorbuy seller made off with over R 100 000-00 from buyers who never received their goods. Whilst many e-commerce sites turn a blind eye, Bidorbuy has taken proactive steps to nip this in the bud. Bidorbuy gave the following account of the recent fraud case: “In a recent isolated case of alleged internet fraud, it is presumed that a seller has gone missing in action after having sold over R100 000's worth of goods on bidorbuy in a single day. The seller has been trading legitimately on bidorbuy for over a year and has previously concluded a number of successful sales with various satisfied buyers.” “In August 2006 he applied to bidorbuy to become a verified seller, and after having passed the stringent velocity tests with bidorbuy he received a verified status. With no previous history or record of abnormal behavior there was no way that bidorbuy could have prevented or suspected any conduct unbecoming.”

**Source: Computer Crime Research Centre, February 16, 2007**

2. **Internet ID theft scam**

The online news site USA Voice isn’t going to win any kudos from media critics. Not for its “news” stories and not for its Fox News-style slogan, “USA Voice: Honest and Unfiltered.” As a phishing scheme, however, privacy experts say it’s a winner. The Web site for the “world’s fastest growing news organization” looked good enough to fool Katherine Brinton, an aspiring journalist in Philadelphia. After posting her resume on Monster.com nine months ago, the 23-year old received an e-mail from USA Voice in November that said it was looking for reporters with “excellent writing skills” and an “innate ability to find the truth.”

**Source: Computer Crime Research Centre, February 20, 2007**

3. **Warning! Online coupon fraud**

Online coupons can be a convenient way to cut costs, but experts warn about potential fraud. NBC 5 reported that crooks sometimes create counterfeit coupons with very high values, and then sell them on the Internet. However, consumers who pay for the tempting deals find out at the register that the coupons are bogus, NBC 5 reported. Connie Yates of Tom Thumb said that consumer should be wary of buying coupons. Experts advise consumers to avoid schemes by patronizing only authorized coupon Web sites.

**Source: Computer Crime Research Centre, February 22, 2007**
http://www.nbc5i.com/money/11076183/detail.html
4. **Pharming scam**

A global financial scam ring attacked more than 65 financial institutions and e-commerce corporations worldwide and stole personal information from these companies using a new hacking technology called “pharming.” Internet security experts and financial circles at home and abroad said yesterday that the hacking first took place in Australia on February 19 and rapidly spread throughout the world, using an average of over 1,000 internet users daily to access sites and steal internet banking IDs and passwords. The U.S. security company “Websense” revealed the above matter on February 22 and those fake sites have been shut down. The list of the companies, which fell victim to the hackers’ attacks, include world famous global corporations such as a British bank Barclays, a Scottish bank, the American Express Card, Discover Card, the world's largest auction site eBay, and the global remittance site PayPal.

**Source:** Computer Crime Research Centre, February 26, 2007

5. **EU to launch scam crackdown**

The European Union will officially launch a crackdown on cross-border scams, including Internet fraud, this week. The scheme, called the Consumer Protection Cooperation Network, is an Europe-wide network designed to help law-enforcement bodies tackle crooks who defraud victims in one country while operating in another. It has been created under the auspices of European legislation called the Consumer Protection Cooperation Regulations, which was passed in 2004. This network of consumer protection watchdogs has been in operation since Dec. 29, 2006, but will be launched officially in Brussels on Thursday by the EU commissioner for consumer affairs, Meglena Kuneva. "Con artists are using mass e-mail or false promises of big earnings to trap vulnerable people," Kuneva said in a statement. "The fraudsters are clever--taking advantage of different legal systems across the EU to target vulnerable people. Their crafty schemes, such as personalizing letters and making them look professional, are costing European consumers millions of euros."

**Source:** ZDNet Asia, Feb 27, 2007
http://www.zdnetasia.com/news/security/0,39044215,61992583,00.htm

**HACK THREAT/INTRUSION**

6. **Chinese police consider releasing hacker's Panda virus fix Would you run a virus writer's anti-virus?**

Experts at SophosLabs™, Sophos's global network of virus, spyware and spam analysis centers, have advised computer users to think carefully about how they remedy virus infections, following news that the Chinese police are to release a clean-up program written by the author of the Fujacks worm. According to media reports from China, authorities are planning to issue a fix to the Fujacks worm which turns icons into a picture of a panda burning joss-sticks. Controversially, the utility has been written by Li Jun, the suspect author of the virus. "Hackers and virus writers have shown themselves to be irresponsible and untrustworthy and I certainly wouldn't choose to run their code on my computer," said Graham Cluley, senior
technology consultant for Sophos. "Additionally, the Fujacks virus left some infected files unable to run. That hardly suggests that the author took quality assurance seriously when he constructed his malware. Our recommendation to computer users would be to clean their PCs with professional tools written by security experts." Chinese police arrested Li Jun, and five other people, in connection with the creation and distribution of the Fujacks worm earlier this week. Li Jun was said in a police statement to have earned more than US $12,500 by selling the malware to other internet hackers. Chinese media have claimed that Li was motivated to create the virus after he failed to find a career in the computer security industry. In the final quarter of 2006 alone, Sophos detected 31,000 different webpages containing versions of the Fujacks malware.


7. **Turkish hacker strikes Down Under**

Legendary Turkish hacker iskorpitx has turned his attention Down Under with an attack that grounded the websites of nearly 600 Kiwi businesses and about 300 international sites hosted by the same US-based web server. As stuff.co.nz reports, "in each case the content of a site's homepage was replaced with an animated medieval knight, Turkish pop music, and a cryptic Turkish message". Vodafone owned ISP ihug was the worst hit, though several other ISPs are also thought to have been involved. The problem affected sites hosted on a US server run by quick.com, the New Zealand subsidiary of which was bought by ihug last year. Only those ihug customers that were inherited as a result of the purchase were vulnerable to the hack. Though the security weakness was supposedly fixed yesterday, many of the affected sites still remain offline, their homepages replaced with the quik internet logo. iskorpitx is estimated to have made about 180,000 attacks in his career, including one that has been labelled the "biggest in history". In this attack he reportedly hacked 21,459 websites in one shot and defaced all with a picture of the Turkish flag and this missive: "HACKED BY iSKORPiTX (TURKISH HACKER) FUCKED ARMANIAN-FUCKED FRANCE-FUCKED GREECE-FUCKED PKK TERROR

Source: The Register, February 16, 2007  
http://www.theregister.co.uk/2007/02/15/iskorpitz_hacks_nz/

8. **Broadband routers welcome drive-by hackers**

Still using the default password that came with that nice broadband router you installed at home? Time to get off your butt and change it: visiting the wrong website is enough to have key settings changed on the most popular models. Symantec warns attackers can employ a simple piece of JavaScript to modify a router's domain name server settings. Once the router is rebooted, a rogue DNS will send the victim to spoofed websites with malicious intent. That could unleash all kinds of new phishing expeditions, Symantec says. For example, the new DNS could route a request for bankofamerica.com or Microsoft's update site to fraudulent sites that steal login details or install back doors.

Source: The Register, February 16, 2007  
http://www.theregister.co.uk/2007/02/15/router_vuln/
9. **Drive-by Web attack could hit home routers**

If you haven't changed the default password on your home router, do so now. That's what researchers at Symantec and Indiana University are saying, after publishing the results of tests that show how attackers could take over your home router using malicious JavaScript code. For the attack to work, the bad guys would need a couple of things to go their way. First, the victim would have to visit a malicious Web site that served up the JavaScript. Second, the victim's router would have to still use the default password that it's pre-configured with out of the box. In tests, the researchers were able to do things like change firmware and redirect a D-Link Systems DI-524 wireless router to look up Web sites from a DNS (Domain Name System) server of their choosing. They describe these attacks in a paper, authored by Sid Stamm and Markus Jakobsson of Indiana University, and Symantec's Zulfikar Ramzan. "By visiting a malicious Web page, a person can inadvertently open up his router for attack," the researchers write. "A Web site can attack home routers from the inside and mount sophisticated... attacks that may result in denial of service, malware infection, or identity theft."

http://www.infoworld.com/article/07/02/15/HNdrivebywebattack_1.html

10. **Hacking business**

Hacking isn't a kid's game anymore. It's big business. Online black markets are flush with stolen credit card data, driver's license numbers, and malware, the programs that let hackers exploit the security weaknesses of commercial software. Cybercriminals have become an organized bunch; they use peer-to-peer payment systems just like they're buying and selling on eBay, and they're not afraid to work together.

Source: Computer Crime Research Centre, February 17, 2007

11. **Imperfect Storm aids spammers**

For 24 hours in mid-January, stock-fraud investigation site StockPatrol disappeared from the internet, overwhelmed by a massive flood of web requests coming from thousands of sources. The attack came after the site wrote a handful of reports investigating and condemning the practice of pump-and-dump stock spam campaigns. No fewer than three botnets targeted StockPatrol, as well as another anti-spam site, and at least five command-and-control servers associated with a different virus, Warezov, according to an analysis released last week. "StockPatrol.com was the victim of a cyberspace assault that evidently was calculated to disable our site and make our reports inaccessible," read a statement posted on 17 January. "In this instance the attack was massive." At the heart of the attack was a single program designed specifically to co-opt victims' computers to aid in sending stock-touting email messages and to participate in denial-of-service attacks - Storm Worm. The program appeared on 19 January and compromised systems by luring their users into opening the attachments of messages with subject lines regarding current news events - including violent storms in Europe. Because the program does not propagate on its own, the name adopted from its subject lines is a misnomer - the Storm Worm is actually a Trojan horse.
12. **Hackers pounce on Howard 'heart attack e-mail'**

Hackers may have captured the login details of around 750 Australian banking customers by circulating a trojan e-mail claiming the prime minister has suffered a heart attack, according to a security company. Titled "John Howard, the current Prime Minister of Australia has survived a heart attack", the e-mail claims Howard suffered the heart attack while at Kirribilli House and is fighting for his life in hospital. The e-mail then provides a link purporting to be an online news report. Users that click the link however are directed to a standard "404 error" page which downloads a trojan to their computer. Joel Camissar, country manager for Websense, which has been tracking the scam, said the trojan monitored infected users' Internet activity. This included logging keystrokes, he said.

**Source: ZDNet Australia, February 21, 2007**
ZDNet AU Internet Security Techmail <members@newsletters.zdnet.com.au>

13. **Monster.com email lure to malicious code**

Websense Security Labs has discovered emails that attempt to lure users to click on a link in order to upgrade their system security. The emails, which are spoofed from Monster, are written in HTML and claim that Monster systems have been upgraded and that users need to download a certified utility to be able to use Monster. The domain name that the emails point to are using five different IP addresses. Upon connecting to one of the IP addresses, the code is run, several files are downloaded and installed on the user's machine, and another file is downloaded and installed from a server in Denmark. The files appear to be designed to steal end-user information.

**Source: Department of Homeland Security, February 26, 2007**

14. **Hackers infiltrate websites**

For the second time in a week, the Delaware County government Web site was infiltrated by a hacker Saturday, causing visitors to the site to see a map of Turkey emblazoned with a bloody sword surrounded by words. The normal operations of the Web site, including the public access to property and court information, were rendered useless as the front page featured images and clusters of Arabic, Hindi and Gujarati words that had no translation. "We will correct it as soon as possible," Delaware County Councilman Michael Puppio said. "Unfortunately, in this age of technology, these things sometimes happen. We'll have to find out how and what it says." By mid-afternoon, Delaware County Executive Director Marianne Grace said county technicians were attempting to bring the Web site down so they could repair it. By 1:30 p.m., visitors were unable to access the site at all.

**Source: Computer Crime Research Centre, February 26, 2007**
15. **Vulnerabilities of WiFi Internet**

They can be found at coffee shops, book stores and hotels. There used to be just a few. Now they are quite literally everywhere. For the technologically savvy, wireless Internet access points -- or WAPs -- make life that much easier. But as News 8 learned, WAPs can also make it that much easier for others to steal people's identities, take their money and generally wreak havoc electronically. David Jacquet is an Internet security expert, an "ethical hacker." During a drive down Congress Street in Portland, his computer sounded off every time it registered a different WAP. He had registered 49 with three blocks to go to News 8's studios.

Source: Computer Crime Research Centre, February 27, 2007

**VIRUS/WORM/TROJANS**

16. **Infected PCs spew malware over 3G connections**

3GSM Much has been written about malware capable of infecting mobile phones, but infected PCs spewing regular malware over 3G connections might be a more serious problem. More firms are using 3G networks for internet backhaul. Corporate machines connecting to these expensive networks often turn out to be infected, according to Michael Coward, chief technology officer of telecoms infrastructure firm Continuous Computing. To prevent PC malware spreading from laptop to laptop across 3G networks, Continuous Computing markets infrastructure technology that allows operators to rapidly deploy next generation networks, which (among other functions) scans mobile traffic for viral code and other crud. As well as PC malware, SMS spam increasingly crops up as a problem. Coward explained that mobile junk messages are a country specific problem with the Philippines, for example, acting as a particular centre of abuse.

Source: The Register, February 16, 2007
http://www.theregister.co.uk/2007/02/15/3g_pc_malware/

17. **Panda virus in China**

China has detained six men in their 20s for writing or profiting from a computer virus dubbed the "joss-stick burning panda" which has infected over a million PCs in the country, local media said on Wednesday. The worm wreaked havoc among individual and corporate users in China in a late 2006 outbreak, deleting files, damaging programs and attacking web portals. It got its name from changing icons on desktops into cute cartoon pandas, the most famous of which holds three burning joss-sticks in his paws. Chinese media have said that the worm was able to steal account names of online gamers and instant messengers, which are holly traded with real money in China's cyberspace.

Source: Computer Crime Research Centre, February 16, 2007
18. **Storm Worm variant targets blogs, bulletin boards**

A variant of the Trojan horse attacks known as Storm Worm emerged Monday, targeting people who post blogs and notices to bulletin boards. Storm Worm emerged in January and raged across the globe in the form of e-mails with attachments that, when opened, loaded malicious software onto victims' PCs, commandeering the machines so they could be used for further attacks. The new Storm Worm variant attacks the machines of unsuspecting users when they open an e-mail attachment, click on a malicious e-mail link or visit a malicious site, said Dmitri Alperovitch, principal research scientist at Secure Computing. But the twist comes when these people later post blogs or bulletin board notices. The software will insert into each of their postings a link to a malicious Web site, said Alperovitch, who rates the threat as "high."

**Source**: CNet News, February 27, 2007-02-28

OTHERS

19. **Quake-hit web links restored in Asia**

Asian telecoms cables damaged in an earthquake late last year have been fully repaired, restoring internet links to the region, Hong Kong authorities announced yesterday. "The earthquakes which occurred near Taiwan on 26 December caused serious damage to six submarine cable systems supporting Hong Kong's external telecoms services," said a spokesman for the Hong Kong government's Office of the Telecommunications Authority. "We are pleased to note that the repair of these cable systems is completed and all our external telecoms services, including internet access, have been fully restored." Two violent magnitude seven quakes in the space of five minutes either directly severed undersea cables, or triggered undersea landslides that buried and broke the data links. Six cables passing around the south east coast of Taiwan were cut, some in more than one location. The links normally carry more than 80 per cent of East Asia's voice and data traffic. In the weeks following the quake, foreign websites loaded very slowly or were even inaccessible for many people in east Asian nations. Websites hosted in the affected areas were equally hard to reach for outsiders. Telephone links were also hit. Repair ships were delayed by winter storms and the difficulty of locating multiple broken sections, but telecoms firms were able to partially restore service by using alternative routes which avoided the broken cables. While the effects of the quake were dramatic, statistically earthquakes rank only slightly above attacks from sharks and other fish as a cause of undersea cable damage, according to data from Alcatel. More than two thirds of all cable damage is caused by fishing trawlers.

**Source**: Department of Homeland Security, February 16, 2007

20. **Computer crime wins the fight**

The head of Britain's Serious Organized Crime Agency says that because of decades of faulty police work, crime kingpins have a one-in-20 risk of prison. Sir
Stephen Lander -- who chairs an organization created 18 months ago by merging several anti-crime agencies -- spoke at a meeting organized by The Times of London. He said the SOCA is still trying to deal with incompatible computer systems and files full of outdated information. "It's because we've not been systematic about capturing that information or going out to find things," Lander said. "So things you would think we would have known we don't." Terry Adams, who allegedly heads a crime syndicate known as the Adams Family with his two brothers, pleaded guilty to money laundering this month and faces a stiff prison term. But Lander suggested Adams is likely to be the exception.

Source: Computer Crime Research Centre, February 18, 2007

21. **FSA has power to order data breach disclosure**

The Financial Services Authority (FSA) could order all regulated financial companies to immediately inform customers of data security breaches, it has said. It has that power, which would largely negate the need for a law ordering notification. Some privacy experts believe that a law ordering notification would make companies more careful and more accountable for the use of personal information, but the financial industry has resisted the calls for legislation. The FSA has told OUT-LAW that it backs notification in almost all cases, but that a blanket rule was not the best option. It said it does have the power to create such a rule, though, which would bind the UK's entire financial services industry to notification. The news comes as Nationwide Building Society, the UK's largest, faces an almost £1m fine for lax security procedures and controls which led to the exposure of the personal details of an unknown number of customers when a Nationwide laptop was stolen. Both the FSA and Nationwide refused to disclose whether or not it ordered Nationwide to inform customers of the security breach.

Source: The Register, February 19, 2007
http://www.theregister.co.uk/2007/02/19/fsa_data_disclosure/

22. **Pirates nabbed**

Police have registered criminal cases against the owners of two computer firms and their four salesmen were also arrested here in Clifton for defying the copyright law, by loading pirated software on new computers. “The installation of unlicensed software CDs onto the hard-disks of personal computers is a crime, no different from theft,” said a Business Software Alliance (BSA) spokesman here today and observed that pirated software is often loaded on new machines in Pakistan “as an incentive for the buyers to purchase the computers from a particular dealer.” Piracy is having an adverse effect on the growth of country’s IT sector with a revenue loss of about US $48 million, he said in a press statement. Compared with the world software piracy rate of 35% and Asia’s 54% in 2005, the software piracy rate in Pakistan was 86%, he said. The spokesman said that all the six accused in the latest raid would now face legal action. While the 41 unlicensed CDs and the two computers loaded with illegal software were also confiscated by the police from their possession, on the complaint of BSA, he added. The police found that the computer hard disks were loaded with many popular computer programmes, including Microsoft XP, MS Office and Norton anti-Virus, besides other software.

Source: Computer Crime Research Centre, February 19, 2007
23. **How cybercrime works**

Hackers are no longer motivated by notoriety – it’s now all about the money. Guillaume Lovet, Threat Response Team Leader at security firm Fortinet, identifies the players, their roles and the returns they enjoy on their investments. This article was contributed to OUT-LAW by Guillaume Lovet. Cybercrime has become a profession and the demographic of your typical cybercriminal is changing rapidly, from bedroom-bound geek to the type of organised gangster more traditionally associated with drug-trafficking, extortion and money laundering. It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that. In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialised skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cybercrime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

*Source: Computer Crime Research Centre, February 20, 2007*


24. **Region faces cybercrime wave**

Cyber criminals are stepping up their focus on the Middle East, as more people go online, experts warned this week. The alert follows the busting last week of an online fraud ring that had been pretending to offer financial services out of the Dubai International Financial Centre (DIFC). David Knott, CEO of the Dubai Financial Services Authority (DFSA), said such attacks are "increasingly" likely here. "The Middle East is becoming a new target for those cyber crimes," Abdulrahman Al-Shenafi, senior adviser on IT and security to the Ministry of Interior in Saudi Arabia told IT Weekly, warning that as more people go online in the region, the more vulnerabilities there would be.

*Source: Computer Crime Research Centre, Feb 22, 2007*


25. **No jail time for child porn**

Despite the arrests each year in Colorado of hundreds of predators who attempt to meet children on the Internet for sex, few of those arrested in stings do any jail time for a first offense. Instead, the majority are sentenced to probation. Internet sex stings, where police pose as children, are resulting in a growing number of arrests here and nationwide. The stings have received a lot of media attention, from the NBC "Dateline" segments that show grown-ups as they arrive for a sex rendezvous with someone they think is a child, to the arrest of Colorado radio personality Scott Cortelyou. And while the arrests often lead to convictions, jail is a different matter.
26. CBI calls for Internet security

Employers’ body the CBI is calling for a national strategy to clarify where responsibility for internet security lies. There are few clear regulations governing online retailers’ liability in protecting their customers from attacks such as phishing and identity theft. How far businesses could or should take responsibility for customers’ security problems is still an open question. But apportioning blame for security issues needs to be done carefully, and an overarching strategy would be more effective than prescriptive regulations, CBI head of e-business Jeremy Beale told the House of Lords Science and Technology Sub-Committee last week. ‘We need a national information security strategy, where educational and training programmes are linked to enforcement capabilities,’ said Beale. ‘There is mutual responsibility, and a clearer framework needs to be formed for where responsibility lies for different actions along the chain.’

27. Security, consolidation top CIOs’ agendas

Despite progress on information technology security, agency chief information officers’ top priorities and concerns are still meeting statutory and regulatory requirements, ensuring data is secure while also available to meet mission needs, and facilitating overall network defense. A survey of 47 CIOs at 33 organizations in the executive, legislative and judiciary branches issued today by the IT Association of America found cybersecurity policies, management and training have improved in the past year, but the execution of cybersecurity remains a major challenge. “IT security has been both their greatest achievement and their biggest challenge,” said Paul Wohlleben, chairman of the CIO survey project and a partner at Grant Thornton. “A lot of CIOs said they feel like they are on an island when it comes to security. They are responsible to make data available but also keep it secure. They need to try to get others in the agency involved.” In its 17th annual CIO survey, ITAA found that many CIOs focus on accomplishing what they have started and not on new projects.